

Недељко Цветковић
cvele1981@gmail.com

**Универзитет у Београду
Факултет политичких наука**



Докторске студије
Отворени докторски семинар

**"Улога и значај тајног надзора комуникације у борби против
тероризма"**

Ментори:
Проф. др Мирољуб Јевтић
Доц. др Марко Вековић

Кандидат:
Недељко Цветковић
бр. индекса 16/2019

Београд, мај 2021.

Улога и значај тајног надзора комуникације у борби против тероризма

Сажетак

Сажетак: Рад се бави анализом тајног надзора комуникација и његовим утицајем на процес неутрализације тероризма. Поступком одређења и дефинисања надзора, уочавају се могућности и значај надзора као средства у процесу супротстављања различитим безбедносним изазовима и ризицима међу којима се налази и тероризам. Затим рад анализира посебне доказне радње чији саставни део представља и тајни надзор комуникација. Анализом процеса одобравања, примене, контроле и поступања са прикупљеним материјалом у току примене тајног надзора комуникације у Републици Србији, а који је строго законски одређен уочава се оквир функционисања, и указује се на неопходност примене ове мере у борби против тероризма. Рад обухвата и елаборацију поступак примене тајног надзора комуникације у Немачкој и Италији. Евалуацијом тајног надзора комуникације у наведеним земљама уочавају се сличности и разлике са спровођењем овог поступка у Србији, као и нове тенденције у поступку спровођења тајног надзора комуникације и поступку неутрализације тероризма. Такође, у раду се анализира и утицај тероризма на процес ограничавања основних људских права која су гарантована како међународним тако и највишим правним актима појединачних држава.

Кључне речи: *надзор, тероризам, посебне доказне радње, тајни надзор комуникација, право на приватност.*

Увод

Настојећи да обезбеди своју сигурност и опстанак, човек је константно вршио прикупљање података о свему што га окружује, затим евалуациом прикупљених података доносио је одлуке које су директно утицале на његов опстанак и развој. У периоду примитивних људских заједница прикупљање података било је поверено појединцима, да би касније настанком организованих људских заједница (држава) овај вид активности почео да добија организован, институционализован карактер.¹

Адекватном прикупљању података од стране организованих институција или појединаца претходи надзор. Надзор често има негативну конотацију, асоцира на тајне истраге и у мислима су нам шпијунски филмови као устаљено мишљење о сагледавању неке или нечије активности. На први поглед чини се да надзор има везе са посматрањем, једна особа посматра другу са циљем остваривања увида у неприкладно и амбивалентно понашање. Затим су ту камере за надзор градова, камере у пословним објектима које могу бележити потенцијално девијантна понашања, која се крећу у распону од непожељних активности до криминалних дела. Међутим надзор се може односити и на непосредно прислушкивање телефона. Наведени примери захтевају примену савремених технологија попут: видео-система за надзор, контролу интернет комуникације, прислушкивање телефона и сл. Имајући у виду наведене техничке могућности, простор за унапређење надзора се последњих година значајно увећао. Информације до којих се дође применом надзора могу се користити као доказ, а у контексту глобалног страха од тероризма чак и поједини необавезни коментари који се могу односити на акте насиља могу бити узети у обзир. Етимолошки, корен речи надзор (*surveillance*, eng.) вуче своје порекло из француске речи "*surveiller*" што значи надгледати.² Надзор се може одредити као низ поступака којима се посебна пажња поклања одређеним појединцима или групама, а који

¹Један од најамбициознијих пројеката министарства јавне безбедности Кине је "полицијски облак" (Cloud). Систем прикупља различите врсте података попут: адресе становања, верске припадности, породичних односа, контроле рађања, боравка у хотелима, употребе авиона, возова, система видео надзора..... Полицијским службеницима свако јутро у осам сати, а на основу локације, систем шаље циљане податке, посебно упозорава на лица која су умешана у тероризам или поступак подривања националне безбедности. Опширније видети: : <https://www.hrw.org/news/2017/11/19/china-police-big-data-systemsviolate-privacy-target-dissen>, приступљено (18.05.2021.).

² Lyon D., *Surveillance Studies: An Overview*, Polity Press, 2007, стр. 13-16.

превазилазе оквири радозналости.³ Значај надзора може се одредити у оквиру координата "да свако ко може одредити време и место на којем ће се неки догађај десити или активност одиграти у великој мери држи ситуацију под контролом".⁴

У својој студији о надзору професор Универзитета Харвард, Дејвид Лајон (David Lyon) износи закључак да је надзор "фокусиран, усмерен, системски одређен, да представља усмерену пажњу на прикупљање личних података, а ради утицаја, усмеравања, управљања и заштите."⁵ Износећи наведену дефиницију Дејвид Лајон (David Lyon) истиче четири аспекта ове дефиниције која проширују наше разумевање о томе шта је надзор и који су његови циљеви. "Прво, надзор је фокусиран на прикупљање информација о појединцима и групама. Друго, надзор мора бити системски уређен, никако произвољан, не сме оставити манипулативни простор. Треће, представља део административног апарата који карактерише савремено уређено друштво - државу, и четврто, надзор има веома широк спектар примене који води суптилном утицају или контроли."⁶

О правној утемељености, значају надзора и временском оквиру у коме може бити примењиван, скоро по правилу, расправља се након реализације терористичких напада и пропуста у раду безбедносних структура.

Посебне доказне радње

Данашње доба, с обзиром на масовно ширење и примену тероризма у политичкој борби, можемо назвати "добом тероризма". Супротстављање овој појави представља један од есенцијалних задатак како појединачних држава, тако и читаве међународне заједнице. Тероризам као вишедимензионална и константно еволуирјућа друштвена појава својим деловањем перманентно настоји да изврши негацију свих вредности савременог друштва. Правовремено детектовање ове негативне друштвене појаве,⁷ намеће држави као носиоцу

³ Исто.

⁴ Исто.

⁵ Richard, Neil M., The Dangers of Surveillance, Harvard Law Review, March 25, 2013, harvardlawreview.org/wp.../pdfs/vol126_richards...

⁶ Исто

⁷ Тероризам је пре свега тајна активност, што онемогућује потпуни увид у деловање овог феномена. Симеуновић, Д., , *Тероризам*, Правни факултет, Београд, 2009, стр. 16.

Симеуновић Д., *Тероризам*, Правни факултет, Београд, 2009, стр. 13.

безбедносног система, да у процесу заштите својих грађана константно врши имплементацију иновираних законских решења којима се омогућује неутрализација тероризма. Посебно место у корпусу мера које се предузимају у циљу спречавања тероризма заузимају посебне докзне радње⁸, посебне мере којима се одступа од неповредивости тајне писама и других средстава општења⁹, односно посебне поступке и мере тајног прикупљања података¹⁰. Посебни поступци и мере којима се врши тајно прикупљање података представљају моћно и истовремено неопходно средство у борби против тероризма. Узимајући у обзир да се у борби против тероризма ове мере показују као *conditio sine qua non*, односно услов без којег се не могу открити, спречити и доказати ова кривична дела, њихова примена представља неопходност".¹¹

Посебне мере тајног прикупљања података су оне мере,¹² које тајно примењују државни органи (превасходно органи безбедности), а чијом применом се ограничавају Уставом загарантована права грађана.¹³ Можемо истаћи да је тајност у прикупљању података фундаментална карактеристика посебних мера, без обзира на основ примене.¹⁴ Примена ових мера врши се пре покретања кривичног поступка, а са циљем откривања структуре, облика, метода деловања и припадника криминалих (терористичких) организација. Циљ примене ових мера је прибављање доказа који ће омогућити покретање кривичног поступка.

Посебне мере могу се поделити у две групе: мере чијим се коришћењем мање или незнатно задире у људска права и слободе. Чине их традиционалне оперативне мере (разговори са лицима, увид у јавне евиденције, прибављање документације и др.), и мере чијом се експлоатацијом у значајној мери ограничавају људска права и слободе (увид у

⁸ Опширније видети: Законик о кривичном поступку, "Службени гласник РС", бр. 72/11, 101/11, 121/12, 32/13, 45/13, и 55/14.

⁹ Опширније видети: Закон о БИА, "Службени гласник РС", бр. 42/02, 111/09 и 66/14.

¹⁰ Опширније видети: Закон о ВБА и ВОА, "Службени гласник РС", бр. 88/09, 55/12 - одлука УС и 17/13.

¹¹ Лечић Б. (2014.), *Европски модели организације и надлежности служби безбедности у сузбијању тероризма*, докторска дисертација, Универзитет у Новом Саду правни факултет.

¹² Према важећем Законик о кривичном поступку у посебне доказне радње се убрајају: тајни надзор комуникације, тајно праћење и снимање, симуловани послови, рачунарск претраживање података, контролисана испорука и прикривени иследник.

¹³ Ђокић К., *Парламентарни надзор над применом посебних мера за тајно прикупљање података у Србији*, Београдски центар за безбедносну политику, 2014, страна 5.

¹⁴ Исто, стр. 5.

садржај свих врста комуникација, статистички подаци о оствареним комуникацијама и др.). У теорији проналазимо и поделу посебних доказних радњи на "мере инфилтрације" које обухватају: ангажовање прикривеног иследника, склапање симулованих правних послова и пружање симулованих услуга, док "мере тајне опсервације" обухватају надзор и снимање телефонских и других разговора и комуникација другим техничким средствима, контрола пословних и личних рачуна осумњиченог и контролисана испорука.¹⁵

Инкорпорација наведених доказних радњи у законску регулативу узрокована је потребама праксе, односно немогућношћу откривања и доказивања тешких кривичних дела као што је тероризам. Кривични поступак који познаје само редовне - класичне радње доказивања постао је неефикасан и недовољан.¹⁶ Први међународни документ који је омогућио имплементацију оваквих мера је Конвенција УН против незаконитог промета опојних дрога и психотропних супстанци из 1988. године - Бечка конвенција.¹⁷ Примена наведених доказних радњи врши се само у случајевима када класичне криминалистичке методе не дају значајније резултате. Селективна примена ових мера узрокована је чињеницом да се њима значајно задире у право на приватност и слободе грађана, те је њихова употреба ограничена поштовањем доказних стандарда у кривичном поступку. Примена посебних доказних радњи могућа је само уз поштовање начела легалитета, супсијадарности и сразмерности, затим постајања основа/основане сумње, примене на основу одлуке суда, временског ограничења примене и контроле над применом мера.¹⁸ Треба истаћи да се пореда наведених ограничења примена доказних радњи врши се само у случајевима када класичне криминалистичке методе не дају значајније резултате.

¹⁵ Лукић Т., *Доказне радње у кривичном поступку*, Правни факултет Универзитета у Новом Саду, Нови Сад, 2011, стр. 25.

¹⁶ Бејатовић С., *Кривично процесно право*, Службени гласник, Београд, 2014., стр. 342.

¹⁷ Скакавац, З., Скакавац, Т., *Кривичнопроцесна регулација посебних доказних радњи у Републици Србији и њихова примена у савременој пракси*, Civitas, Београд, бр.7/2 - 2017 године, 2017, стр.39- 40.

¹⁸ На основу препоруке садржане у Резолуцији донетој на XVI kongresu AIDP-a., XVI међународни конгрес за казнено право 2/1999б, 1051.

Тајни надзор комуникација

Динамичан развој техничких средстава којима се може вршити прислушкивање, дешава се скоро сваким даном, упоредо са развојем комуникационих средстава. У употреби се налазе сателити, рачунари са пратећим програмима који региструју одређене, задате речи (које најчешће могу фигурирати у извршењу терористичких, криминалних или других безбедносно интересантних активности). Затим компјутерски програми након регистрације само тачно одређене речи, се усмеравају на слушање и снимање. Окончањем поступка снимања, овако прикупљен материјал даље је предмет обраде различитих програма и аналитичких служби безбедности. Наведене околности праћене константном еволуцијом организованог криминала и тероризма наметнуле су држави као носиоцу система безбедности да константно иновира у процесу друштвене контроле криминала. Наведеној контроли значајан допринос даје тајни надзор комуникације. Тајни надзор комуникација представља, надзор и снимање комуникације која се обавља телефоном или другим техничким средствима, електронске или дуге адресе осумњиченог и заплону писама и других пошти. Овај надзор обухвата и комуникацију која је остварена разменом порука преко мобилних телефона, различитих апликација за размену порука и путем електронске поште.¹⁹ Најзначајнија својства тајног надзора комуникације су: тајност, да се његовом употребом ограничавају уставом загарантована права (право на приватност) и кривично процесна неупотребљивост доказног материјала прикупљеног на овај начин у колико је у току поступка одобрења и преимене дошло до кршења законом одређеног поступка примене.²⁰ Област тајног надзора комуникације регулишу кривично процесни закони и закони којима се регулише рад служби безбедности.²¹ Последње одређивање и нормирање тајног надзора комуникације у Р Србији извршено је Закоником

¹⁹ Кршић, Ж., *Криминалистички и кривично процесни аспекти тајног надзора и снимања комуникација у Босни и Херцеговини Зборник радова*, XVII Дани криминалистичких наука, Међународна научна конференција, Crimen, Forensis, Securitas, Сарајево 5-6 октобар, 2017, стр. 276.

²⁰ Британско законодавство представља главни изузетак у Европи, информације које су прикупљене пресретањем комуникације на територији Велике Британије, а чију примену одобрава само министар унутрашњих послова, могу бити употребљене само у обавештајне сврхе - не прихватају се као доказни материјал (али информације које се прикупе пресретањем комуникације у иностранству може бити употребљено пред Британским судовима.) Опширније видети: <https://rm.coe.int/deployment-of-special-investigative-means-srb/16807828f9>, приступљено 13.05.2021.

²¹ Лечић, Б., *Улога и значај посебне доказне радње тајног надзора комуникација у истрази кривичног дела тероризма*, Civitas, Београд, број 7/2 - 2017, стр. 98.

о кривичном поступку 2011. године, наведена област је регулисана од 166. члана до 171. члана. Како истиче М. Шкулић, а према Законик о кривичном поступку Р Србије, примена ове посебне доказне радње могућа је ако су испуњени општи материјални услови за примену посебних доказних радњи и формални услови. "Одредбе о овој посебној доказној радњи обухватају њено одређивање, спровођење, проширење и достављање извештаја и материјала"²². На образложени предлог јавног тужиоца суд одређује надзор и снимање комуникација које се обављају путем телефона и других техничких средстава, електронске адресе или заплену писама и поштом чиме се испуњује формални услов.²³ Наредба коју доноси судија за предходни поступак садржи: расположиве податке о лицу према коме се тајни надзор комуникације одређује, законски назив кривичног дела, означање телефонског броја или адресе осумњиченог, односно телефонског броја или адресе за које постоје основи сумње да је осумњичени користи, разлоге на којима се заснива сумња, начин спровођења и трајање ове посебне доказне радње.²⁴ Одређивање временског рока трајања тајног надзора комуникације врши се на два начина: 1) фактичким роком чије је деловање засновано на *ultima ratio* својству ове посебне доказне радње, што се своди на обавезу прекидања спровођења надзора чим престану разлози за његову примену, и 2) одређивањем посебних максималних рокова формалне природе (одређених у месецима) у оквиру којих се може примењивати ова мера.²⁵ Примена тајног надзора комуникације може трајати три месеца, а због неопходности даљег прикупљања доказног материјала, тајни надзор комуникације може се продужити највише за још три месеца. Уколико се тајни надзор комуникације примењује због кривичних дела за чије је процесуирање надлежно јавно тужилаштво посебних надлежности, тајни надзор комуникације се може продужити највише још два пута у трајању од три месеца што представља максималну могућност експлатације ове посебне доказне радње у трајању од

²² Илић Г., Матић Бошковић М., *Посебне мере тајног прикупљања података у кривичном поступку: поглед из правосуђа*, Београдски центар за безбедносну политику, 2015, страна 9.

²³ Опширније видети: М. Шкулић, *Кривично процесно право, седмо измењено и допуњено издање*, Правни факултет Универзитета у Београду, Београд, 2014, стр. 243–244.

²⁴ Шкулић М., *Посебне доказне радње у функцији сузбијања тероризма и основни правни аспекти против терористичког деловања војних снага*, Правни факултет, Универзитет у Београду, 2017, DOI: 10.5937/vojdol1606275S

²⁵ Исто, стр. 282.

дванаест месеци.²⁶ Наредбу о тајном надзору комуникације у Републици Србији је на основу законских овлашћења омогућена је: Безбедносно-информативној агенцији (БИА); Војнобезбедносној агенцији (ВБА); и Министарству унутрашњих послова.²⁷ О поступку спровођења тајног надзор комуникације сачињавају се дневни извештаји, који се заједно са прикупљеним снимцима комуникације и писмима и другим пошиљкама о оствареној комуникацији осумњиченог достављају судији за претходни поступак и јавном тужиоцу на њихов захтев.²⁸ Узимајући у обзир велике могућности и значај тајног надзора односно вредности података прикупљених на овај начин, као и чињеницу да се применом ових мера задире у Уставом загарантована права, неопходно је онемогућити злоупотребе развојем механизма за контролу. Законодавство у Србији познаје три екстерна актера, која у оквиру својих надлежности врше контролу над применом посебних мера: 1) контрола коју спроводи Народна скупштина Републике Србије²⁹, 2) контрола коју спровode судови³⁰, 3) контрола коју спровode независни државни органи (НДО), које представљају Заштитник грађана и Повереник за информације од јавног значаја и заштиту података о личности, (само у оквиру својих овлашћења).³¹ Одређени надлежни државни орган који наредбом спроводи тајни надзор комуникација, дужан је да сачињава дневне извештаје о спровођењу исте. Дневни извештаји се достављају судији за претходни поступак и јавном тужиоцу на њихов захтев. Истеком рока у коме је вршена примена посебне доказне радње, овлашћени државни орган за њену примену дужан је да достави судији за претходни поступак извештај о примени и припадајући прикупљени материјал (снимке, документацију). Изузетак представља извештај о примени контролисане испоруке који се доставља Републичком јавном тужиоцу (извештај о примени контролисане испоруке доставља се јавном тужиоцу).

²⁶ Опширније видети: Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције.

²⁷ Лазих Р., *Контрола служби безбедности у Србији*, Академија за националну безбедност и ЈП "Службени гласник", Београд, 2014, страна 174.

²⁸ Опширније видети: Законик о кривичном поступку, "Службени гласник РС", бр. 72/11, 101/11, 121/12, 32/13, 45/13, и 55/14.

²⁹ Основ контроле је Закон о основама уређења служби безбедности Републике Србије, а надзор спроводи Одбор за контролу служби безбедности.

³⁰ Судска контрола врши се у два правна режима: на основу Законика о кривичном поступку и на основу Закона о службама безбедности.

³¹ Надлежност чине: људска права и законитост и правилност у раду органа управе.

Уколико у року од шест месеци од момента упознавања јавнога тужиоца са садржајем прикупљених материјала, исти не буде искоришћен за покретање кривичног поступка или уколико тужаоц изјави да га неће користити у поступку, судија за претходни поступак дужан је да донесе решење о уништавању прикупљеног материјала. Прикупљени материјал се уништава под надзором судије за претходни поступак који о томе сачињава записник.³²

Примена тајног надзора комуникације у Немачкој и Италији

Електронски надзор комуникација у Немачкој се врши на основу Закона Das Gesetz über die Beschränkung des Post- und Fernmeldegeheimnisses aus dem Jahre 1968. и Das Strafprozessordnung – StPO (Закон о кривичном поступку). Електронски надзор комуникација се предузима у превентивном смислу ради очувања националне безбедности, а у репресивном смислу, у циљу утврђивања извршилаца каталошки одређених кривичних дела, када за то постоји основана сумња, предвиђено чланом 100а поменутог закона.³³ Надзор над комуникацијама може бити кориштен и ради утврђивања боравишта осумњиченог лица које се налази у бекству. Одобравање мере у превентивне сврхе врши Начелник БНД-а, односно начелник војнообавештајне службе безбедности. За репресивне сврхе меру одобрава суд на основу предлога надлежног државног тужиоца. Изузетак представља случај хитности, тада меру може одобрити и државни тужилац уз накнаду потврду суда, ова процедур је предвиђена чланом 100б - наведеног закона. Временско трајање мере је ограничено на три месеца, уз могућност проширења за још три месеца. Контрола над спровођењем мера може се вршити административно, судски и парламентарно.³⁴ Потребно је истаћи да Немачко законодавство разликује "прислушкивање" које се одвија у оквиру стана осумњиченог и када осумњичени борави ван њега. Примена тајног надзора комуникације у оба случаја могућа је само у случају

³²Опширније видети: члан 163. Законика о кривичном поступку, "Службени гласник РС", бр. 72/2001, 101/2011, 121/2013, 32/2013, 45/2013 и 55/2014.

³³Опширније видети: http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html, приступљено 19.05.2021.

³⁴Ничић Ж., *"Надзор комуникација као мера процесне принуде"*, безбедност полиција грађани бр.1-2, 2014. стр. 96-98.

каталожки набројаних тешких кривичних дела, укључујући чланство у терористичким организацијама или пружање подршке истим.³⁵ Примена мера у оквиру стана могућа је наредбом коју издаје веће кога чине три судије регионалног суда, за кривична дела из националне безбедности. Од ове мере изузети су лекари, правници и свештенство, осим ако се не сумња да су учествовали у наведеном кривичном делу. Примена мера у оквиру стана осумњичених ограничена је на временски период од четири недеље, уз могућност проширења на још четири недеље, што је регулисано чланом 100ц.³⁶ Пресретање комуникација која се остварује преко мобилног телефона, или мејл адресе и лоцирање оптужених, остварује се уз логистичку помоћ оператера телекомуникационих услуга³⁷, а на основу наредбе суда. Када разлози хитности то налажу, налог о пресретању комуникација може донети јавно тужилаштво чију наредбу у року од три дана мора потврдити суд - судија. Након испуњења законских услова телекомуникациони оператер дужан је да успостави услове којима се омогућује пресретење комуникација осумњиченог. Како истиче Шкулић Немачко законодавство разликује више врста аудио и видео надзора: 1) надзор и снимање телекомуникација, 2) прислушкивање и снимање разговора који се воде у станovima и другим просторијама, 3) прислушкивање и снимање техничким средствима разговора који нису намењени јавности, а воде се изван стана, 4) прибављање података о контактима путем средстава телекомуникација, 5) тајна присмотра уз тајно фотографисање и видео-снимање, 6) утврђивање броја прикључка мобилног телефона и броја коришћења СИМ картице.³⁸ Модели примене тајног надзора комуникација и поступак спровођења наведених су различити, заједничко им је да сви облици имају законски оквир поступка одобравања, спровођења и контроле примене.

³⁵Станковић М., *Посебне доказне радње у функцији сузбијања организованог криминала у Републици Србији*, докторска дисертација, Универзитет привредна академија у Новом Саду правни факултет за привреду и правосуђе у Новом Саду, 2020, стр. 178-179.

³⁶ Исто, стр. 179.

³⁷ Глобализација чији је једини покретач профит створила је мноштво проблема у овој области. Поједини оператри телекомуникационих услуга у Канади и Француској нису били спремни да пруже своје услуге безбедносном сектору, уколико им за њихове услуге не буде плаћено. Пресретнута комуникација од стране оператера је била шифрована, овакав начин односа међу овим субјектима озбиљно је ометао спровођење истрага. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf, приступљено 13.05.2021.

³⁸ Шкулић М., *Посебне доказне радње у функцији сузбијања тероризма и основни правни аспекти против терористичког деловања војних снага*, Правни факултет, Универзитет у Београду, стр. 286, DOI: 10.5937/vojdol1606275S.

У борби против тероризма, поред тајног надзора комуникације италијанском законодавству су на располагању: прекоранични надзор, прикривене активности, информатори, контролисана испорука, надзор, претраге и симуловани послови. Сви облици деловања морају бити прописани и регулисани законом о кривичном поступку или другим законом. Пресретање комуникација представља праћење комуникација остварених путем телефона, е-поште и разговоре између осумњичених лица на неком месту. Мера се може примењивати у истражне сврхе и у току кривичног поступка. Доказни материјал прикупљен на овај начин може бити кориште као доказ на суду.³⁹ Пресретање телефонских разговора⁴⁰, комуникације путем е-поште, и разговора између особа које су физички присутне на неком месту у превентивне сврхе, а у контексту борбе против етероризма омогућено је чланом 5 Закона број 438/2001, кад год се процени да је ова мера неопходна у неутралисању кривичног дела тероризма.⁴¹

Такође правни основ за примену мере надзора комуникација у Италији чини и Антимафијашки закон Codide Antimafia No. 203 из 1991.године. Мера се примењује у репресивне сврхе, у циљу истраживања тешких кривичних дела, која су одређена каталогом кривичних дела уз услов постојања јаких индиција. У случајевима постојања сумње за постојање мафијашке делатности, за примену ове мере на основу Антимафијашког закона није потребно постојање јаких индиција.⁴² Наведено добија на значају последњих деценија, са обзиром на изразиту повезаност организованог криминала и тероризма нарочито у процесу "прања новца".

Надзор комуникација у превентивне сврхе представља тзв. административно прислушкивање, одобрава суд за спречавање мафијашког криминалног деловања, на

³⁹ De Koster, P., *Terrorism: special investigation techniques*, Strasbourg Cedex, Council of Europe Publishing, pg.163, 2005, стр. 189.

⁴⁰ Због немогућ идентификације припејд корисника мобилних телефона и корисника рачунара у инетрнет кафеима (што озбиљно отежава и успорава истаргу), италијански пружоци телекомуникационих услуга од 2007. године, дужни су да воде регистар корисника оваквих услуга, појединим регистрима је могућ електронски приступ. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf, приступљено 13.05.2021.

⁴¹ Станковић М., *Посебне доказне радње у функцији сузбијања организованог криминала у Републици Србији*, докторска дисертација, Универзитет привредна академија у Новом Саду правни факултет за привреду и правосуђе у Новом Саду, 2020, стр. 182.

⁴² Лукић, Т., *Електронски надзор комуникација као метод прибављања доказа за кривична дела организованог криминала*, Зборник, Правни факултет, Нови Сад, 1/2005, 2005, стр. 249-260.

образложени предлог начелника ДИА и уз сагласност министра унутрашњих послова. Док меру у репресивне сврхе одобрава суд на предлог државног тужиоца, изузетак представљају случајеви хитности (до 24 часа), меру може одобрити начелник МУП-а, уз накнадно прибављено одобрење суда. Тајни надзор комуникације према одредбама ЗКП-а се одређује до 15 дана, односно 40 дана уз могућност сукцесивног продужавања мере у периодима од по 20 дана по налогу суда на основу Антимафијашког закона. Када се мера предузима у превентивне сврхе временски се ограничава на 20 дана уз могућност продужења.

Утицај тероризма на ограничавање основних људски права

Адекватност одговора тероризму често одређују два критеријума, прихватљивост општим демократским принципима и успешност у решавању проблема. Мере које могу бити успешне често су неприхватљиве ("претварање једне земље у полицијску државу"), док са друге стране испољене мере, прихватљиве нашим демократским принципима, су неуспешне (када се лицима повезаним са тероризмом обезбеди пуна заштита демократског система).⁴³ Након окончања судског пороцеса у Милану на слободу је пуштено пет исламиста који су били оптужени за учешће у тероризму. Судија Clementine Forleo проценила је да прикупљање новца и регрутовање особа у Италији са циљем њиховог упућивања у Ирак, а ради борбе против припадника међународних снага безбедности представља легалан чин. Правдајући одлуку да овакве активности представљају герилско деловање и позивајући се на Глобалну конвенцију УН-а о тероризму.⁴⁴ Поједини релевантни стручњаци из ове области искључиву предност дају репресивном начину супротстављања, са тенденцијом умањења значаја демократских одговора, док са друге стране имамо заговорнике помирења и компромиса, који сматрају да репресија не утиче на смањење, већ њена употреба расплињава тероризам.

⁴³ Sederberg, P. C., "Global Terrorism: Problems of Challenge and Response". - In: Kegley, Charles W. Jr., *The New Global Terrorism*, 2003, стр. 267-284.

⁴⁴ Марковић, С., *Тероризам и друга кризна стања савременог друштва и њихов утицај на ограничавање људских права и демократија*, 2009, <https://hrcak.srce.hr/87000>, приступљено 15.05.2021.

Као фактор са посебним утицајем наспрам прихватљивости и успешности појављује се време, које веома често представља ограничавајући фактор. Решења која су прихватљива на краћи временски период не морају бити успешна на дужи период и обрнуто. Савремене тенденције у борби против тероризма приоритет дају превенцији, што доводи до решавања проблема пре његовог ескалирања. Једна од мера која даје значајан допринос, која је најчешће експалтише и која се преузима превентивно, у борби против тероризма представља тајни надзор комуникација. Међутим применом тајног надзора комуникација од стране безбедносног сектора врши се делимично ограничавање основних људских права - право на приватност. Ексклузивитет права на приватност препозната је и усвојен 1948. године Унивезалном декларацијом о људским правима од стране УН.⁴⁵ Овај пример следила је и Европа 1950. године у којој је постојање и поштовање овог права потврђено усвајањем Европске конвенције о заштити људских права и основних слобода.⁴⁶ Борба против тероризма неминовно "укључује размену између наших вредности и безбедности"⁴⁷. Представља изазов у изналажењу одговора који успешно излазе на крај са тероризмом, али при томе минимално оштећују наше вредности."⁴⁸ На вечитој клацкалицы демократских друштава налазе се приватност и безбедност. Преме мишљењу Европског суда за људска права, а у складу са члановима 6 и 8 Европске конвенције о људским слободама и правима, посебне доказне радње умеђу којима се налази и тајни надзор комуникација су неопходне уколико се на адкватан начин жели супротставити свим облицима организованог криминала и тероризма.⁴⁹ С тим у вези можемо истаћи да тајни надзор комуникације представља легитимну меру у процесу откривања најтежих кривичних дела, нарочито оних која се уобичајеним процесним средствима не могу доказати због сложености и високог нивоа конспиративности

⁴⁵The Universal Declaration of Human Rights, <http://www.un.org/en/universaldeclaration-human-rights/>, приступљено 17.05.2021.

⁴⁶European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf, приступљено 17.05.2021.

⁴⁷Према члану 8. , ставу 2., "Јавне власти неће нарушавати право на приватност сем ако то није у складу са законом и ако је неопходно у демократском друштву, у интересу националне безбедности, јавне безбедности или економске добробити земље, а ради спречавања нереда или криминала, заштите здравља и морала, или заштите права и слободе других", Опширније видети: <https://rm.coe.int/deployment-of-special-investigative-measures-srb/16807828f9>, приступљено 13.05.2021.

⁴⁸David, C., The New Global Terrorism, "The Four Waves of Rebel Terror and September 11", 2002, стр. 271.

⁴⁹Скакавац, З., Скакавац, Т., *Кривичнопроцесна регулација посебних доказних радњи у Републици Србији и њихова примена у савременој пракси*, Civitas, Београд, бр.7/2 - 2017 године, стр. 42.

извршилаца.⁵⁰ Тероризам као константно еволуирајућа друштвена појава, која користи све благодети техничко технолошког развоја, а коју прати изразито повећање бруталности и шокантности у процесу манифестовања, изскује константо иновирање у поступку неутрализације. Поједине чланице ЕУ након низа напада на својој територији, притиска јавности и политичке елите имплементирале су различита законска решења којима се проширују овлашћења безбедносног сектора. Указано се огледа у у примеру Француске која је непосредно након терористичких напада у Паризу безбедносном сектору омогућили низ мера које проширују надзор над грађанима. Нови закон омогућује да безбедносни сектор без претходног одобрења суда сагледава дигиталне и мобилне комуникације осумњичених за везе са тероризмом, затим омогућено је вршење претрес кућа и објеката осумњичених, без сагласности суда, изузетак представљају стамбени објекти судија, тужиоца и адвоката. Као техничка мера издваја се деактивација свих интернет налога који промовишу тероризам и екстремизам. Немачки модел борбе против тероризма је свом безбедносно-обавештајном сектору омогућио да покреће истраге против лица и организација умешаних у терористичку делатност само на основу иницијалних сумњи. Затим италијанско законодавство омогућује службама за борбу против тероризма да осумњичене за терористичко деловање без налога задржавају у притвору до 24 часа, и саслушавају их без присуства правних браниоца. Такође им је омогућено да без сагласности осумњичених узимају узорке ДНК, косе и пљувачке у циљу откривања идентитета лица.⁵¹

Иако је исходиште примене ове мере ефикасно супротстављање савременим формама манифестовања организованог криминала и тероризма, неопходно је заштитити демократске тековине, од злоупотребе овог моћног средстав. Проширење овлашћења и његово погрешно схватање односно несавесна примена води у злоупотребу, као начин превазилажења ових замки намеће се потреба унапређења постојећих система контроле примене тајног надзора комуникације-података. "Држава мора контролисати и чувати

⁵⁰Пауновић, Н., *Тајни надзор комуникације као легитиман основ за одступање од права на приватност личности са освртом на праксу европског суда за људска права*, <https://www.harmonius.org/wp-content/uploads/2020/01/Pages-from-Harmonius-2019-15.pdf>, приступљено 17.05.2021.

⁵¹Лечић Б., *Европски модели организације и надлежности служби безбедности у сузбијању тероризма*, докторска дисертација, Универзитет у Новом Саду правни факултет, 2014, стр. 370.

своје чуваре, како би била сигурна да они адекватно поступају."⁵² Како истиче Салаи леганост у поступку ограничавања права на приватност постиже се формирањем законског оквира који је јавно доступан, јасан и прецизан на начин да сваки заинтересовани појединац може увидом у законски квир утврдити ко је и на који начин овлашћен спроводити надзор. Прецизност законодавног оквира одликује се у спецификацији категорија особа или кривичних дела које могу бити стављене под надзор, временског рока у ком се надзор може спроводити, те временског рока чувања и располагања сакупљеним подацима. Наведени захтеви - циљеви представљени су као захтев предвидљивости.⁵³

Закључак

Терористичке активности постају све сложеније, испољавање које је препуштено машти њихових инспиратора и организатора нужно захтева константно прилагођавање и изналажење нових начина и мера у супротстављању овој друштвеној појави. Тенденција динамичних промена у начину деловања, избора циљева, одабиру средстава и мета терористичких организација наметнула је држави и међународној заједници доношење нових законских прописа који ће омогућити унапређење рада постојећих и формирање нових "тела", пре свега органа извршне власти, чија адекватна употреба омогућује ефикасну борбу против тероризма. Улога и значај надзора у процесу очувања безбедности несумњиво су доказана кроз историју⁵⁴. Посебно на значасу ова мера добија последњих неколико година динамичним технолошким развојем комуникационих средстава. Свршено манифестовање надзора који је уоквирен у законску процедуру огледа се у примени посебних доказних радњи, међу којима се налази и тајни надзор комуникације, као једна од најчешће примењиваних мера у поступку детекције тероризма. Представници власти држава, односно наднационалне организације (ЕУ) у кризним

⁵²Игњатовић, Д., *Мере пресретања комуникације и задржавања података из перспективе Стразбура и прописа и праксе у Републици Србији*, Београдски центар за безбедносну политику, Београд, 2015, стр. 23.

⁵³Салај З., *Међународноправне импликације масовног надзора електричних комуникација у контексту људских права с посебним освртом на сигурносно-обавештајни систем у Републици Хрватској*, <https://hrcak.srce.hr/196201>, приступљено 17.05.2021.

⁵⁴Кинески војни теоретичари истицали су важност обавештења коју је доносила претходница (извиђачи) још у VI веку п.н.е., сматрајући да је предзнање један од битних услова за постизање војних и политичких циљева.

ситуацијама, након реализације терористичких напада траже од својих надлежних институција хитну и одлучну реакцију која неутралише тероризам. Стањем угрожености након терористичких напада се оправдава употреба ванредних мера које излазе из стандардних политичких поступака са циљем неутралисања безбедносне претње⁵⁵. Ограничавање основних људских права које се врши применом тајног надзора комуникације мора бити у складу са законском регулативом. Дерогација права на приватност могућа је уз примену начела начела легалитета, супсијадарности и сразмерности. На крају можемо закључити да примена тајног надзора комуникације омогућује долазак до квалитетних, поузданих и благовремених података, чиме се остварује простор за правовремену реакцију контраобавештајних, обавештајних, полицијских, војних и на крају правосудних органа. Овакав след околности има за циљ неутралисање или уништење терористичких активности чему тежи свака држава.

Литеатура

1. Бејатовић С., (2014.), Кривично процесно право, Службени гласник, Београд,
2. De Koster, P. (2005). Terrorism:special investigation techniques, Strasbourg Cedex, Council of Europe Publishing, pg.163,
3. Ђокић К. (2014.), Парламентарни надзор на применом посебних мера за тајно прикупљање података у Србији, Београдски центар за безбедносну политику,
4. Игњатовић, Д.,(2015.), Мере пресретања комуникације и задржавања података из перспективе Стразбура и прописа у Републици Србији, Београдски центар за безбедносну политику, Београд,
5. Илић Г., Матић Бошковић М., (2015),Посебне мере тајног прикупљања података у кривичном поступку: поглед из правосуђа, Београдски центар за безбедносну политику,
6. Кршић, Ж., (2017). Криминалистички и кривично процесни аспекти тајног надзора и снимања комуникација у Босни и Херцеговини Зборник, радова XVII Дани криминалистичких наука, Међународна научна конференција, Crimen, Forensis, Securitas, Сарајево 5-6 октобар, 2017,

⁵⁵Више о томе видети: *UK spy agencies need more powers, says Cameron*, <https://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks>, приступљено 17.05.2021.

7. Лечић Б. (2014.), Европски модели организације и надлежности служби безбедности у сузбијању тероризма, докторска дисертација, Универзитет у Новом Саду правни факултет,
8. Лечић, Б., (2017). Улога и значај посебне доказне радње тајног надзора комуникација у истрази кривичног дела тероризма, *Civitas*, Београд, број 7/2 - 2017,
9. Лукић Т., Доказне радње у кривичном поступку, Правни факултет Универзитета у Новом Саду, Нови Сад, 2011.,
10. Lyon D., (2007.), *Surveillance Studies: An Overview*, Polity Press,
11. Ничић Ж. (2014.), "Надзор комуникација као мера процесне принуде", безбедност полиција грађани бр.1-2,
12. Richards Neli M. (2013.), *The Dangers of Surveillance*, Harvard Law Review,
13. Sederberg, P. C.,(2003.),"Global Terrorism: Problems of Challenge and Response". - In: Kegley, Charles W. Jr., *The New Global Terrorism*,
14. Симеуновић Д. (2009.), Тероризам, Правни факултет, Београду,
15. Скакавац, З., Скакавац, Т.,(2017). Кривичнопроцесна регулација посебних доказних радњи у Републици Србији и њихова примена у савременој пракси, *Civitas*, Београд, бр.7/2 - 2017 године,
16. Станковић М., (2020), Посебне доказне радње у функцији сузбијања организованог криминала у Републици Србији, докторска дисертација, Универзитет привредна академија у Новом Саду правни факултет за привреду и правосуђе у Новом Саду,
17. Шкулић М., Кривично процесно право, седмо измењено и допуњено издање, Правни факултет Универзитета у Београду, Београд, 2014.,
18. Шкулић, М., (2016). Посебне доказне радње у функцији сузбијања тероризма и основни правни аспекти противтерористичког деловања војних снага, *Војно дело*, бр.6/2016,
19. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције. Службени гласник Републике Србије, бр. 94/2016.,

Нормативно правна регулатива

1. Устав Републике Србије, „Сл. гласник РС“, бр. 98/06.,
2. Закон о основама уређења служби безбедности Републике Србије. „Сл. гласник РС“ бр.116/07, 11.12.2007. године.,
3. Законик о кривичном поступку, "Службени гласник РС", бр. 72/11, 101/11, 121/12, 32/13, 45/13, и 55/14.,
4. Закон о БИА, "Службени гласник РС", бр. 42/02, 111/09 и 66/14.,
5. Закон о ВБА и ВОА, "Службени гласник РС", бр. 88/09, 55/12 - одлука УС и 17/13.,
6. Закон о заштитнику грађана, "Службени гласник РС", бр.79/05 и 54/07.,
7. Закон о слободном приступу информација од јавног значаја, „Сл. гласник РС“, бр. 120/04 и 54/07.,
8. Закон о заштити података о личности", Службени гласник РС, бр. 97/2008.,

Интернет извори

1. <https://www.undoc.org/documents/organized-crime/Law-Enforcement/Electronic-surveillance.pdf>,
2. <https://hrcak.srce.hr/87000>,
3. <https://www.harmonius.org/wp-content/uploads/2020/01/Pages-from-Harmonius-2019-15.pdf>,
4. The Universal Declaration of Human Rights, <http://www.un.org/en/universaldeclaration-human-rights/>,
5. European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf,
6. <https://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-america-paris-attacks>,
7. <https://hrcak.srce.hr/196201>,
8. http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html,
9. <https://www.hrw.org/news/2017/11/19/china-police-big-data-systemsviolate-privacy-target-dissen>,

The role and importance of covert surveillance of communication in the fight against terrorism

Summary: The paper deals with the analysis of secret surveillance of communications and its impact on the process of neutralization of terrorism. The process of defining and defining surveillance reveals the possibilities and importance of surveillance as a means in the process of confronting various security challenges and risks, including terrorism. Then the paper analyzes special evidentiary actions, an integral part of which is the secret surveillance of communications. The analysis of the process of approving, applying, controlling and handling the collected material during the application of secret surveillance of communications in the Republic of Serbia, which is strictly determined by law, shows the framework of functioning, and indicates the necessity of applying this measure in the fight against terrorism. The paper also includes an elaboration of the procedure of application of secret surveillance of communication in Germany and Italy. The evaluation of secret surveillance of communication in the mentioned countries shows similarities and differences with the implementation of this procedure in Serbia, as well as new tendencies in the procedure of conducting secret surveillance of communication and neutralization of terrorism. Also, the paper analyzes the impact of terrorism on the process of restricting basic human rights that are guaranteed by both international and the highest legal acts of individual states.

Keywords: surveillance, terrorism, special evidentiary actions, covert surveillance of communications, right to privacy.